

REMARKS

The Office Action of August 10, 2005, has been received and its contents carefully reviewed. By the above Amendment, Applicants have amended claims 1, 37, and 73 to more distinctly highlight the features of the present invention. Claims 1-75 remain pending in the application. No new matter is introduced by this Amendment. (See, e.g., pg. 6, paras. [0063] – [0065], and pg. 10, para. [0101], of Applicants' Published Application). Thus, Applicant respectfully submits that no new matter is presented by entry of this Amendment and that the application is in condition for allowance.

The rejection of claims 1-72 under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. 6,574,609 to *Downs et al.* is respectfully overcome, because *Downs* fails to disclose, teach or suggest all of the features recited in the pending claims. For example, independent claim 1, as amended (emphasis added), recites:

A system for distributing digital documents having usage rights associated therewith, said system comprising:
a server having at least one digital document stored thereon;
a client computer having a standard application program including a rendering engine capable of being accessed to render content;
a communications network coupled to said client and said server; and
a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions for accessing the rendering engine, wherein the security module is separate from the rendering engine.

Similarly, independent claim 37, as amended (emphasis added), recites:

A method for distributing digital documents having usage rights associated therewith, said method comprising:
storing at least one digital document on a server;
requesting, over a communications network, the at least one digital document from a client computer having a standard application program including a rendering engine capable of being accessed to render content; and
enforcing security conditions for accessing the rendering engine with a security module which is downloaded and included in said client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions, wherein the security module is separate from the rendering engine.

Thus, independent claims 1, and 37, as amended, include the novel features of a security module which is downloaded to and included in a client computer, the security module being adapted to be attached to the standard application program for enforcing security conditions while being separate from the rendering engine. In addition, independent claims 1 and 37

specifically recite that the client computer has a standard application program which includes a rendering engine capable of being accessed to render content.

By contrast, *Downs* is directed to a conventional digital rights management (DRM) system employing secure containers, but fails to disclose, teach or suggest all of the features recited in independent claim 1 and 37. In particular, *Downs* specifically requires that the end-user device include a Player Application which is implemented on the end-user device by installation with software and/or consumer electronics hardware. (col. 11, lines 54-60). In particular, the Electronic Digital Content Store downloads the Player Application to the end-user device. (Col. 22, lines 9-12). The End-User Player Application is specifically required to be installed on the end-user device, and includes many of necessary security features. For example, the Player Application cryptographically scrambles the Content before storing it in the end-user device, and generates a scrambling key for each Content item. (Col. 2, lines 36-40). Thus, only the Player Application that is knowledgeable of the embedding algorithm and the associated scrambling key is able to read or modify the embedded data. (Col. 20, lines 53-55). In addition, the Player Application running on the end-user device is responsible for soliciting license authorization from the Clearinghouse. (Col. 22, line 60-63). There is no suggestion whatsoever in *Downs* that his system may be implemented on a client computer that has a standard application program which includes a rendering engine capable of being accessed to render content, as is recited in the claims. Accordingly, Applicants respectfully submit that independent claims 1 and 37, as amended, are allowable over *Downs*.

Further, the present invention recited in independent claims 1 and 37 includes recognition of problems discovered with respect to conventional digital rights management (DRM) systems, such as the system of *Downs*, for example, as described at page 2 of Applicants' Published Application:

[0014] The second approach is to utilize proprietary formats wherein the document can only be rendered by a select rendering engine that is obligated to enforce the publisher's rights. Of course, this approach requires the use of a single proprietary format and loses the ability to combine plural popular formats and the richness of content associated therewith. Further, this approach requires the user to use a proprietary rendering application that must be obtained and installed on the user's computer and requires development of the rendering application for each format to be rendered in a secure manner. Further, the documents must be generated or converted using non-standard tools.

The present invention recited in independent claims 1 and 37, advantageously, addresses the discovered problems with respect to conventional DRM systems, such as the system of *Downs*, for example, as described at page 6 of Applicant's Published Application:

[0063] The preferred embodiment utilizes a standard rendering engine of an application program, such as a browser, a word processor, or any other application or display program. The preferred embodiment achieves this by interfacing with the application and standing between the application and the document to control access to the document. Accordingly, a separate proprietary rendering engine for each document format is not required. Further, any data format supported by the application will be supposed by the invention without modification. It can be seen that the preferred embodiment permits DRM systems to be adapted to standards, such as TCP/IP and the use of browsers to render HTML. Further, the preferred embodiment facilitates various functionality that permits DRM to be applied to systems in a manner that is transparent to the user. Several examples of methods of operation of document distribution system 200 are described below.

By contrast, *Downs* fails to disclose, teach or suggest the noted features recited in independent claims 1 and 37, nor recognize or address the discovered problems with conventional DRM systems. Accordingly, one of ordinary skill in the art would find no motivation to arrive at the invention recited in independent claims 1 and 37, based on *Downs*, absent improper hindsight reconstructions of Applicants' invention based on Applicants' disclosure.

Dependent claims 2-36 and 38-72 are allowable over *Downs* on their own merits and for at least the reasons as argued above with respect to their independent claims.

The rejection of claims 73-75 under 35 U.S.C. § 102(e), as being anticipated by U.S. Patent No. 6,311,269 to *Luckenbaugh et al.* is respectfully overcome, because *Luckenbaugh* fails to disclose, teach or suggest all of the features recited in the pending claims. For example, independent claim 73, as amended (emphasis added), recites:

An HTML document adapted to be rendered by Web browser in a secure environment, said document comprising:
an HTML header defined between header tags;
an HTML body containing content; and
security information embedded in said header, said security information being associated with one or more usage rights.

Thus, independent claim 73, as amended, includes the novel features of an HTML document having security information imbedded in an HTML header, the security information being associated with one or more usage rights. By contrast, *Luckenbaugh* is directed to the use of a “cookie” assigned to the HTML header portion of an HTML document. (Col. 2, lines 40-44). According to *Luckenbaugh*, a “cookie” is a “passive group of data, generally randomly assigned and may be stored in a file at the user’s browser.” (Col. 2, line 58-63). The cookie may be used as a “security cookie” to verify a user’s credentials. (Col. 3, line 42-63). There is no suggestion whatsoever in *Luckenbaugh* to embed security information associated with usage rights in an HTML header. Accordingly, Applicants respectfully submit that independent claim 73, as amended, is allowable over *Luckenbaugh*.

Further, the present invention recited in independent claim 73 and discussed on page 10 of Applicants’ Published Application provides that:

[0101] In the example above, the title of the HTML page is “MY BOOK” which will be rendered in accordance with standard HTML rules. The signature is a number as an attribute of the header and will not be rendered but can be culled for security purposes. In step 1608, the reply is sent to security module 237 of client computer 230. In step 1610, security module 237 analyzes the security information in the reply header and passes content of document 222 to browser 232 for rendering in accordance with the usage rights described by or associated with the security information.

By contrast, *Luckenbaugh* fails to disclose, teach or suggest the noted features recited in independent claim 73. In addition, one of ordinary skill in the art would find no motivation to arrive at the invention recited in independent claims 73, based on *Luckenbaugh*, absent improper hindsight reconstructions of Applicants’ invention based on Applicants’ disclosure.

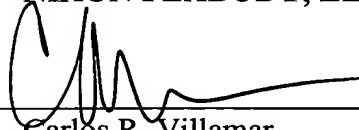
Dependent claims 74-75 are allowable over *Luckenbaugh* on their own merits and for at least the reasons as argued above with respect to their independent claims.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. However, if the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the

undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

NIXON PEABODY, LLP

A handwritten signature in black ink, appearing to read 'Carlos R. Villamar', is written over a horizontal line.

Carlos R. Villamar
Reg. No. 43,224

Date: November 10, 2005

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080